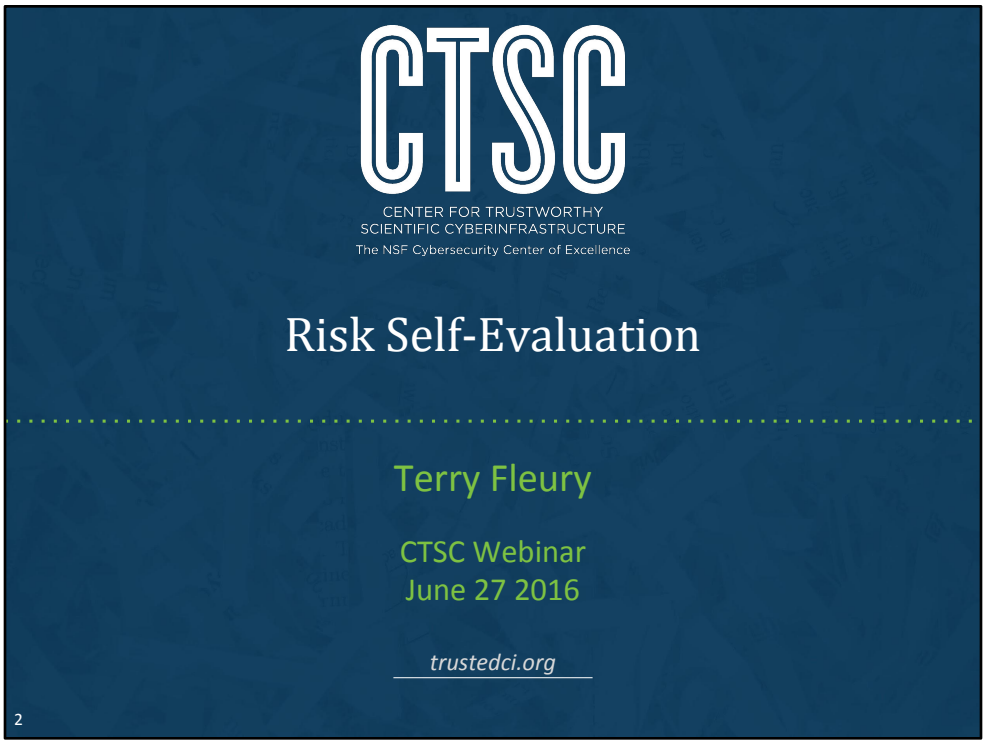
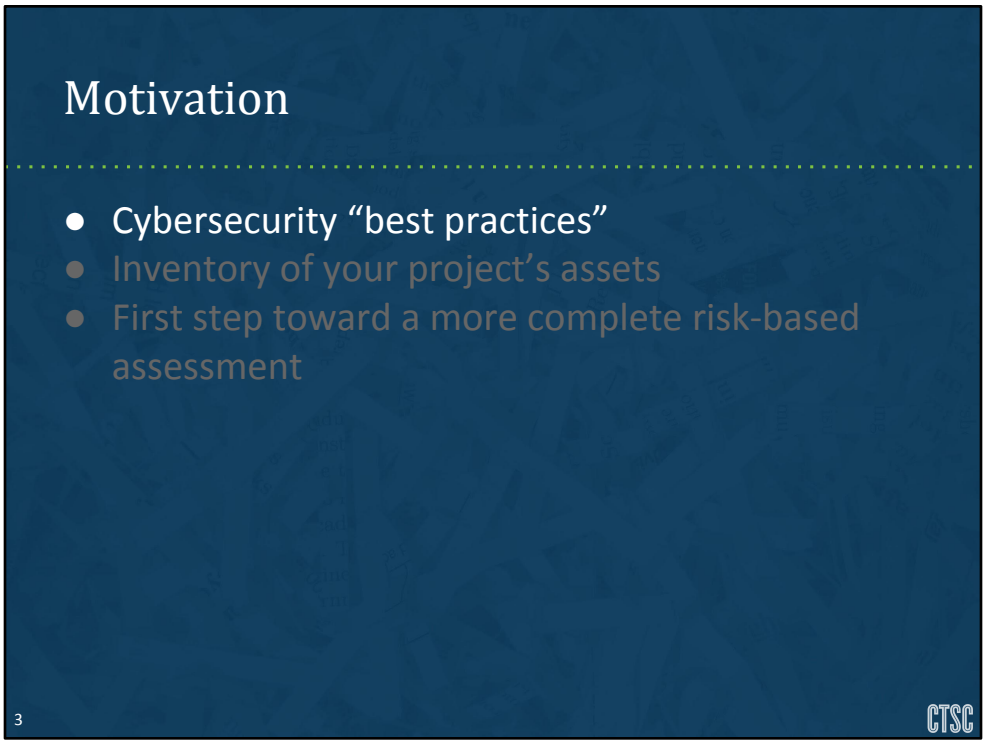
(Jeannette to give opening remarks here.)



Hello. My name is Terry Fleury. Thank you for tuning in for my short presentation on Risk Self-Evaluation.

First, a little bit about myself. For the past 11 years, I have been a “research programmer” in the Cybersecurity Directorate at the National Center for Supercomputing Applications at the University of Illinois. My current software development projects involve Identity and Access Management solutions for CILogon and SWAMP, the Software Assurance Marketplace.

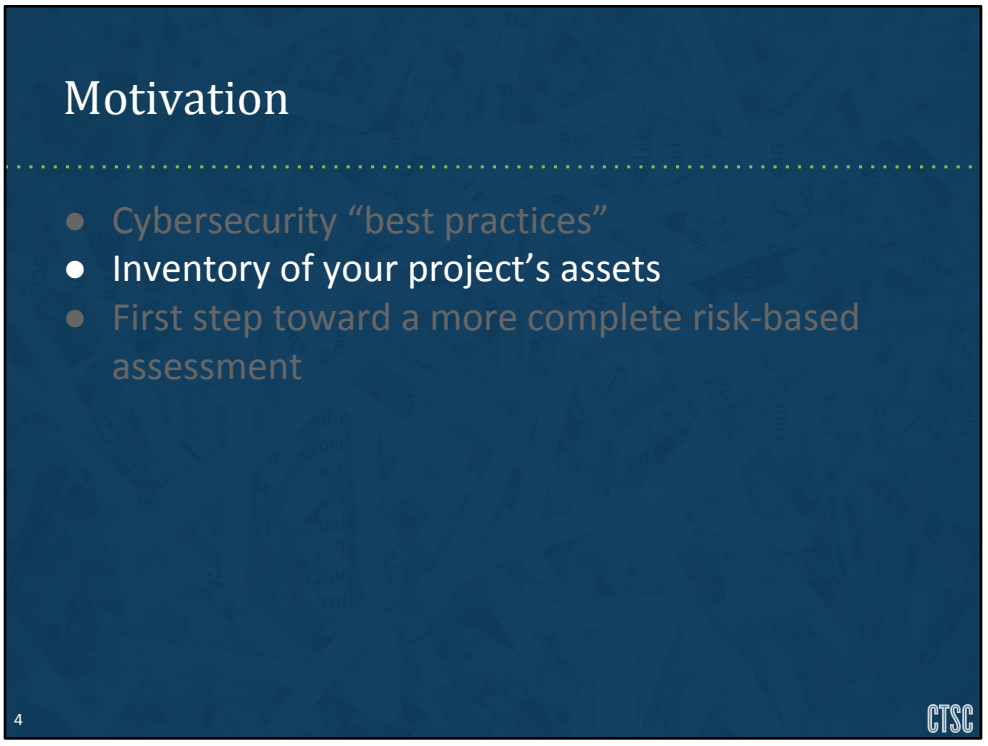
I have worked with CTSC since its inception three years ago. During that time, I have assisted several projects with developing various aspects of their cybersecurity programs. In these engagements, I have used the Risk Self-Evaluation spreadsheet which I will discuss in this presentation.



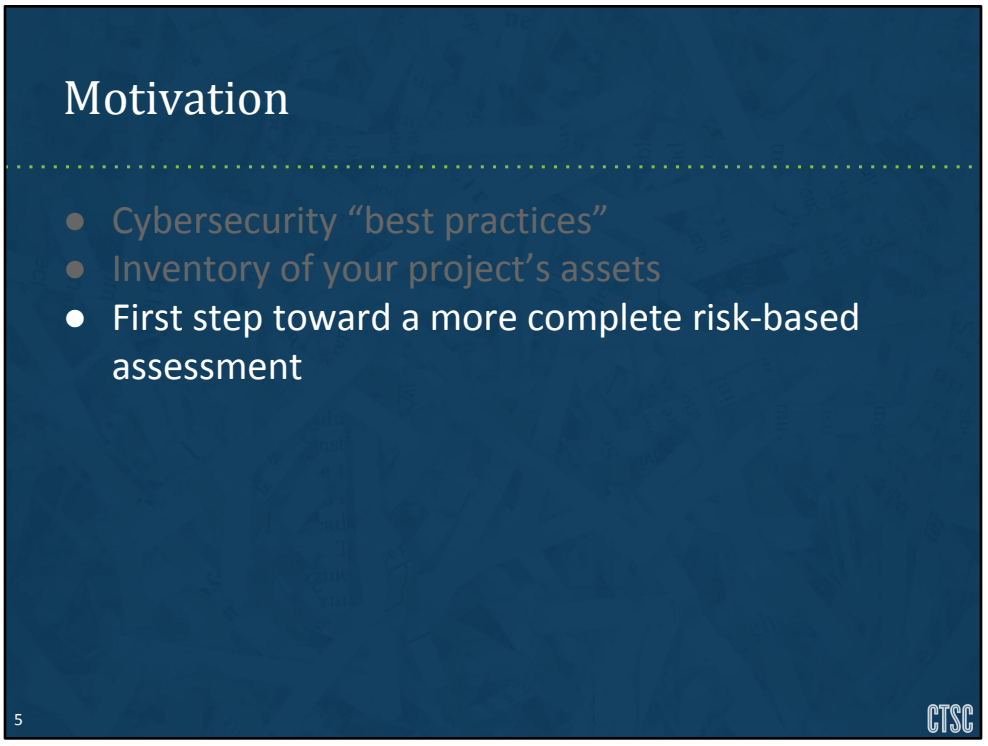
So why would a project be interested in performing a Risk Self-Evaluation? At its root, good cybersecurity involves employing “best practices” that have been used to secure computer systems for years. These “best practices” include things such as:

- making sure software is patched with the latest security updates;
- securing networks so that the minimum set of ports are open;
- monitoring access and alerting on intrusions;
- managing administrator access to important systems; and
- basic identity and access management for your project.

There is no “magic bullet” for cybersecurity, but if you can implement “best practices” as described in the Risk Self-Evaluation, you will handle 80%-90% of your risk.



Another reason for doing a Risk Self-Evaluation is to pull together a complete inventory of your project’s assets. The inventory will include not only your physical systems such as servers and networks, but also the software used by your project, as well as the people working with your project. As you will see in the first section of the Risk Self-Evaluation, implementation of policies and procedures apply not just to your systems, but also to your staff.



Finally, if your project is required to perform a complete risk-based assessment such as the type described in NIST 800-30 or ISO 27005, filling out the Risk Self-Evaluation spreadsheet is an excellent first step toward a performing broader risk assessment.

Personally, I have found the Risk Self-Evaluation extremely useful in my previous work with CTSC engagements which ultimately lead to a more complete risk-based assessment. Asking projects to fill out the spreadsheet has spurred engagees to think critically about their assets and potential risks to their project, and has also given CTSC staff a starting point to discuss details about the project’s systems and processes.

The basis for the Risk Self-Evaluation is the document “Securing Commodity IT in Scientific CI Projects”, which is available on the trustedci.org website. Feel free to download it for your reference. The content of this document comes from the TeraGrid project all the way back in 2004, and yet the risks described in the document still apply today. This goes back to what I said about applying “best practices” for computer security, which have been around for years.

The first section of the document gives a brief overview. The remaining sections describe risks and potential controls which can be applied to mitigate the risks.

The Risk Self-Evaluation spreadsheet is simply a conversion of the Securing Commodity IT document into spreadsheet form, with additional columns to allow you to note if your project has addressed the risks noted. This spreadsheet is a Google Sheet with public view-only access. If you want to make entries in the spreadsheet, you must first make a copy of the spreadsheet by going to the “File” menu and selecting “Make a copy” or “Add to My Drive”. Of course, this requires that you have a Google account, which is free. Alternatively, you can download the spreadsheet as a Microsoft Excel document for editing on your local computer.

Spreadsheet Layout

Section	Risk	Goal	Recommended Control	Mitigated?	Comments
POLICY AND PROCEDURES					
2.1	Poor credential management by users can lead to compromise by an attacker.Resources can be used for unacceptable/illegal purposes.	Ensure users are aware of their responsibilities when using IT resources.	Have a published acceptable use policy that all users are required to accept and uphold.		

CTSC

So let's get into the spreadsheet itself. The spreadsheet has rows describing risks and potential mitigating controls. These rows are divided into sections as in the Securing Commodity IT document. Here you see the first section for "Policy and Procedures".

Spreadsheet Layout

Section		Goal	Recommended Control	Mitigated?	Comments
	URES				
2.1	Poor credential management by users can lead to compromise by an attacker.Resources can be used for unacceptable/illegal purposes.	Ensure users are aware of their responsibilities when using IT resources.	Have a published acceptable use policy that all users are required to accept and uphold.		

CTSC

Across the top of the spreadsheet, the column headers are as follows. The Section column corresponds to the section number in the Securing Commodity IT document. Note that the section numbers start at 2.1 since section 1 in the document is the Introduction. The section numbers have no other special connotation, meaning that the risks are not necessarily ordered, say from worst to best.

Spreadsheet Layout

Section	Risk	Goal	Recommended Control	Mitigated?	Comments
POLICY AN					
2.1	Poor credential management by users can lead to compromise by an attacker.Resources can be used for unacceptable/illegal purposes.	Ensure users are aware of their responsibilities when using IT resources.	Have a published acceptable use policy that all users are required to accept and uphold.		

CTSC

The next column is the Risk in question. These are common risks which apply to cyberinfrastructure. The risk could be the loss of an asset, or simply the problem of dealing with an unknown. Note that some risks may not apply, depending on the size and scope of your project. There is an entry in the Mitigated column to reflect this.

Spreadsheet Layout

Section	Risk	Goal	Recommended Control	Mitigated?	Comments
POLICY AND PROCEDURES					
2.1	Poor credential management by users can lead to compromise by an attacker.Resources can be used for unacceptable/illegal purposes.	Ensure users are aware of their responsibilities when using IT resources.	Have a published acceptable use policy that all users are required to accept and uphold.		

CTSC

Next we have the Goal column. This column lists the related security goal we wish to achieve by mitigating the risk in question. The Goal description serves to provide better insight into the relation between the Risk and Recommended Control columns.

Spreadsheet Layout

Section	Risk	Goal	Recommended Control	Mitigated?	Comments
POLICY AND PROCEDURES					
2.1	Poor credential management by users can lead to compromise by an attacker.Resources can be used for unacceptable/illegal purposes.	Ensure users are aware of their responsibilities when using IT resources.	Have a published acceptable use policy that all users are required to accept and uphold.		

CTSC

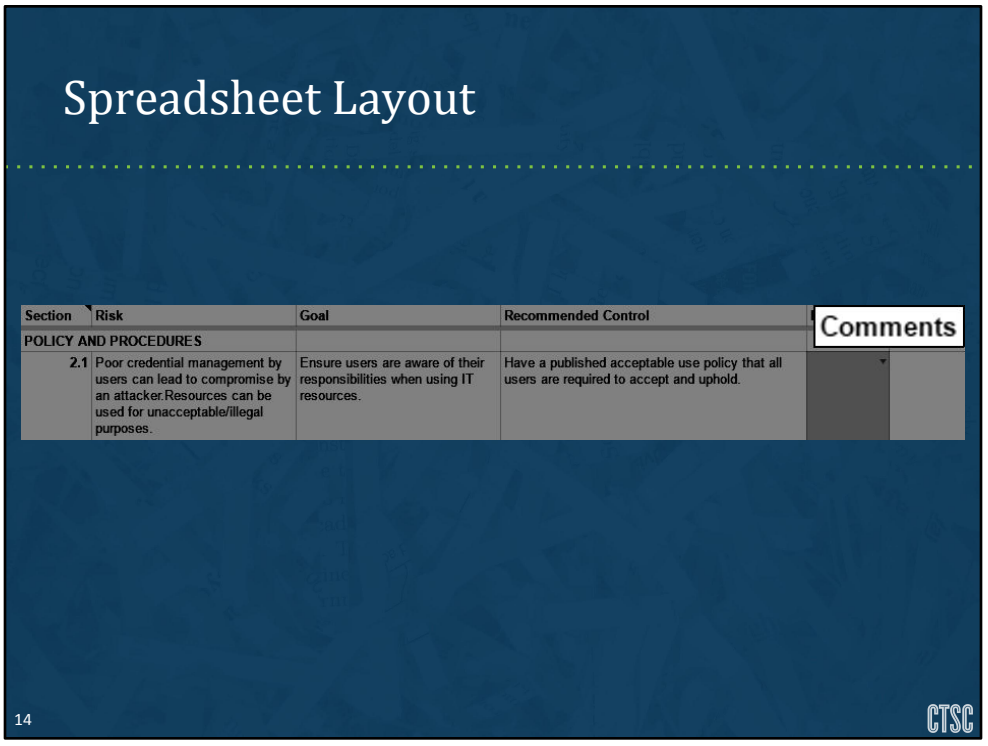
The Recommended Control column describes actions that a project can take to mitigate the risk in question. Note that there may be many controls which could be applied to mitigate the risk. These Recommended Controls are general in nature. Your project may have other controls in place. Keep that in mind when filling in the next column.

Spreadsheet Layout

Section	Risk	Goal	Recommended Control	Mitigated?
POLICY AND PROCEDURES				
2.1	Poor credential management by users can lead to compromise by an attacker.Resources can be used for unacceptable/illegal purposes.	Ensure users are aware of their responsibilities when using IT resources.	Have a published acceptable use policy that all users are required to accept and uphold.	

CTSC

The Mitigated column is one of the two columns that you need to populate when filling out the spreadsheet. I'll describe this column in detail in a minute.



Finally, the Comments column is the other column you need to populate when filling out the spreadsheet. You should consider the potential audience for the completed spreadsheet when filling out this column. If you think others in your project would benefit from this spreadsheet, you may want to give detailed information about the reason behind the answers in the Mitigated column, as well as potential actions that should be taken, and by whom. On the other hand, if the spreadsheet is just for your own personal use, then maybe you can make short notes to yourself about potential actions. Ultimately, the spreadsheet is simply a tool to help you evaluate the risks that may apply to your project, and how to mitigate those risks. It is up to you how you use this tool.

So, getting back to the Mitigated column. When you double-click on a cell in this column, you will be prompted to select one of the following answers: Yes, Partial, No, N/A, or Unknown.

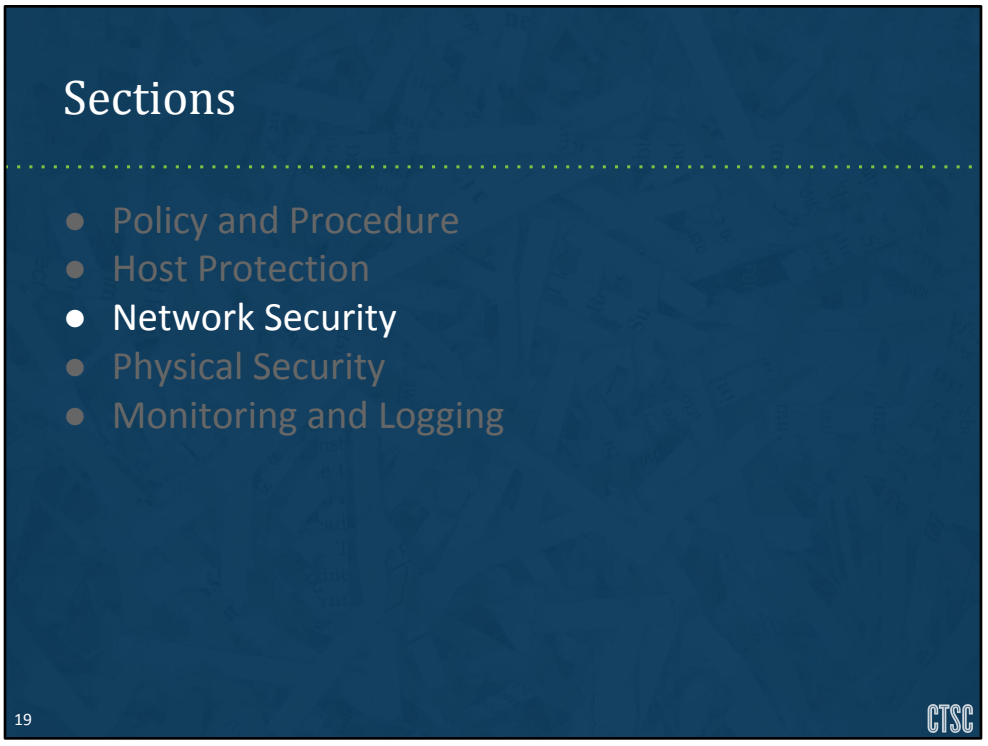
- Select “Yes” if you are certain that you have measures in place to mitigate the risk described. You may optionally include text in the Comments column to describe the type of mitigation, especially if it differs from the text in the Recommended Control column.
- Select “Partial” to indicate that you have some solution in place to mitigate the risk in question, but the solution does not address all aspects of the risk. In the Comments column, document what you currently have in place, and what further controls you think would be needed to change the Mitigated column to a “Yes” response.
- Select “No” if the risk has no mitigation factors in place, and document the reason why in the Comments column.
- Select “N/A” if the risk described is not applicable to your project.
- Note that selecting “Unknown” is a perfectly acceptable response. Part of filling out the Risk Self-Evaluation

- spreadsheet is learning about the types of risk that may affect your project. You may be learning about a particular risk for the first time, in which case it is natural not to know if your project has mitigation measures in place for the risk. The logical solution would be to find out if the risk applies, and if so, what is currently being done to mitigate that risk. Use the Comments column to document who may be able to provide answers.

As stated previously, the spreadsheet is divided into sections based on the Securing Commodity IT document. I won't describe every risk listed in the spreadsheet, but I will give a summary of the sections. The first section is about Policies and Procedures. These are documented processes that apply to your computer hardware and software, as well as your staff and users. Examples include the following:

- Make sure users know their responsibilities when using project resources. Think End User License Agreement.
- Make sure your staff members know about these documented policies and procedures.
- Keep an updated inventory of your project's resources.
- Document how to respond to security issues and recover from any damage.

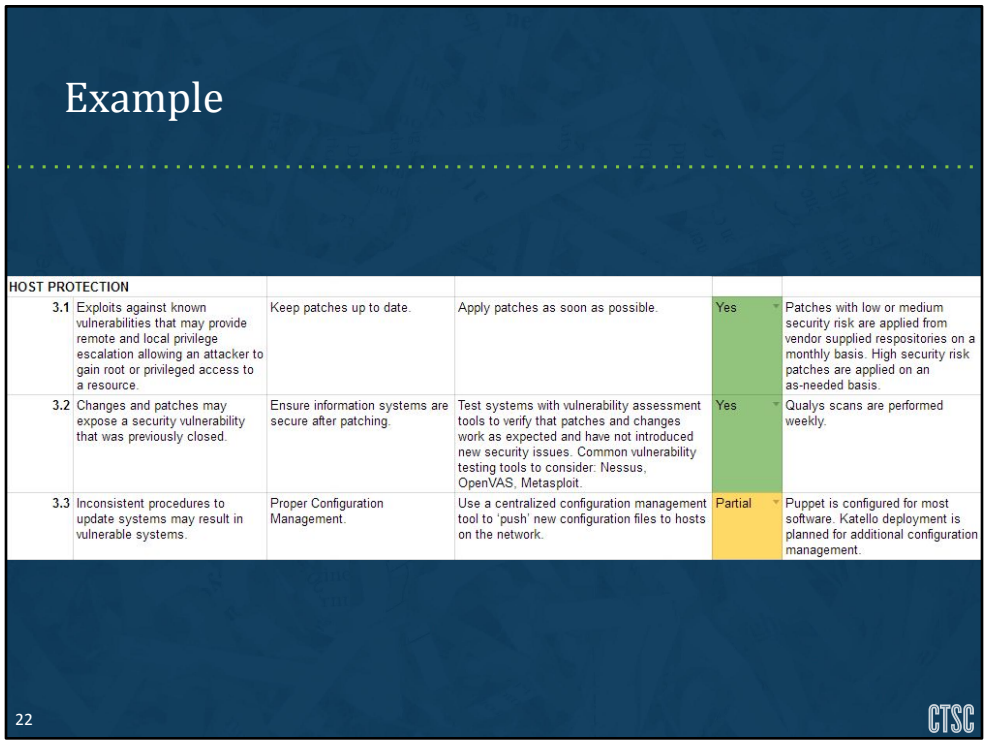
The Host Protection section centers on providing security to your compute resources. This includes topics such as software patches, configuration management, limiting number of and access to essential services, credential protection, and system accounting and logging.



The Network Security section points out potential risks to your network and how to address those risks. Examples include monitoring network traffic, and management of your project's network devices. If your project does not manage any networking subsystems, you should at least be aware of the network solutions provided to your project and how those networks are secured, if at all.

The Physical Security section addresses access to your resources, i. e., locks on doors and computer racks. Again, if your project does not actually have any compute resources which you manage directly, you should at least be aware of how the provided compute resources are physically accessed so you have an understanding of the risk.

And finally, the Monitoring and Logging section discusses the importance of maintaining system and network logs in order to investigate security incidents. While this is a potentially deep area of discussion, just a few items are listed. For example, centralized logging prevents intruders from erasing their malicious activities.



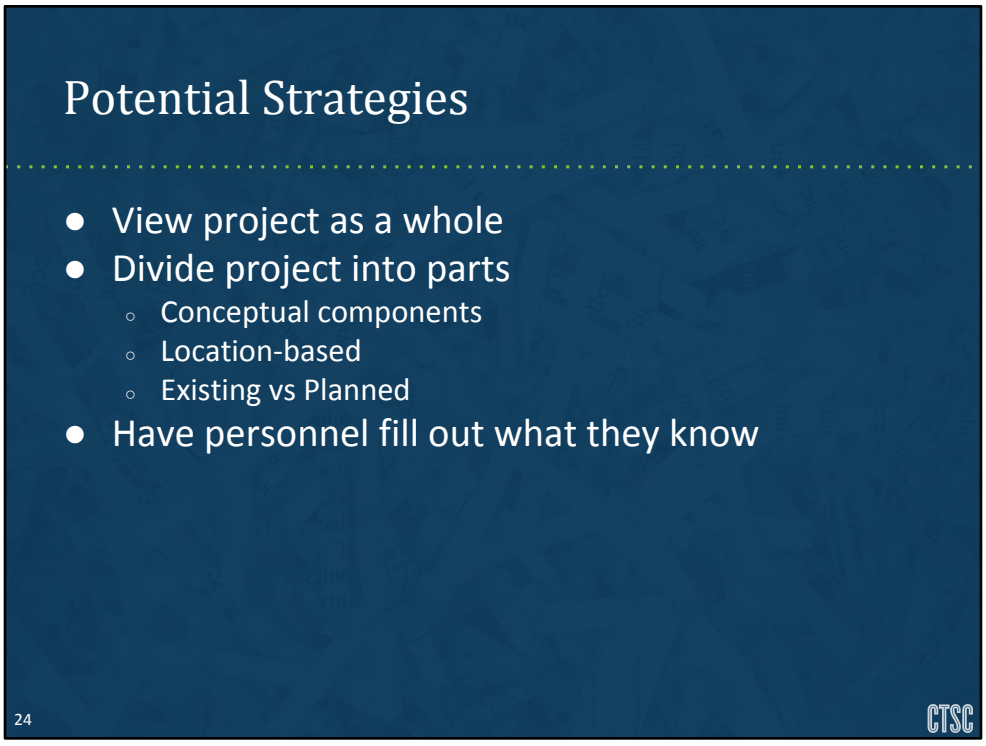
As an example, I have filled out a few entries from the “Host Protection” section. As you can see, the Mitigated column entries are automatically color-coded based on the answer you choose. Green for Yes, Yellow for Partial, Red for No, etc. This allows you to quickly see the risks that apply to your project that need to be addressed.

Risk 3.1 describes the risk associated with outdated software. The recommended control is basically to apply patches in a timely manner. If your software is provided by a vendor, this may simply be a matter of maintaining a consistent system update schedule. If you have custom software, you may need to subscribe to mailing lists to make sure you are notified of updates. In the example here, all software packages on my systems are provided by CentOS, and thus I simply do monthly O/S updates. However, I also subscribe to the CentOS-announce mailing list to look for packages which have been updated due to high security risk bugs. In that case, I update the affected packages in a more timely fashion.

Risk 3.2 discusses the use of vulnerability management software to ensure that any security issues are discovered quickly so that they

can be dealt with. Here I note that I use Qualys to scan my network for common vulnerabilities on a weekly basis.

Risk 3.3 is about configuration management. In the Mitigated column, I selected Partial. In the Comments column, I note that I currently use Puppet to push out configuration settings for most of the software installed on my systems, but not all. I further note that Katello is in the works which will provide additional capabilities for installing and configuring software from a centralized server. If I come back to this spreadsheet for a re-evaluation in the future, I would note the Yellow box and verify that I had deployed a configuration management solution involving Katello.



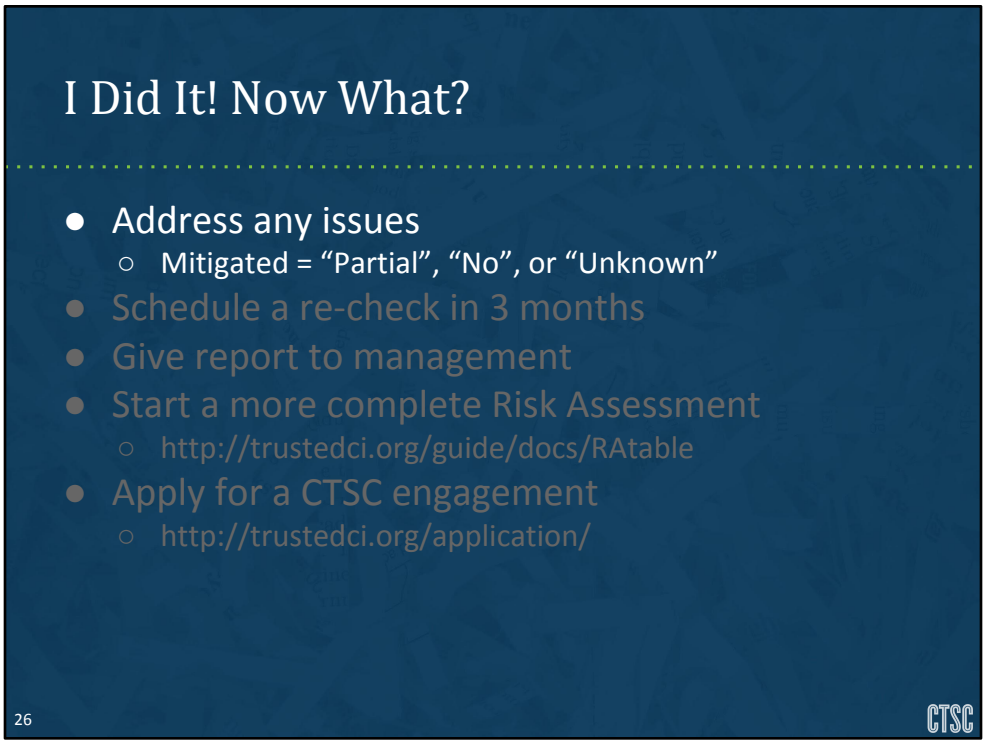
When you first read through the Securing Commodity IT document and the associated Risk Self-Evaluation spreadsheet, you may find it difficult to fill out. There are a few strategies you could employ. If your project is small, you could simply view all assets of the project as a whole, applying the risks listed in the spreadsheet across your project resources.

If your project is large, this solution may not be feasible. In that case, you may need to fill out multiple copies of the spreadsheet, with each copy targeting a different part. The way you divide up your project will be dictated by several factors.

- If your project shares some resources, but not others, you may be able to divide your project up based on conceptual components.
- If your project is geographically diverse, it might be useful to fill out multiple spreadsheets, one for each physical location.
- If your project is currently in development, with some operational components and others that are planned for the future, create separate spreadsheets for existing and planned

- aspects of the project.

The last strategy is useful if you personally don’t have the information necessary to fill out many parts of the spreadsheet. In this case, make multiple copies of the spreadsheet and give them to the people who DO have the information. Ask them to fill out as much as they can in their area of expertise. Then you can compile all responses into a single spreadsheet.



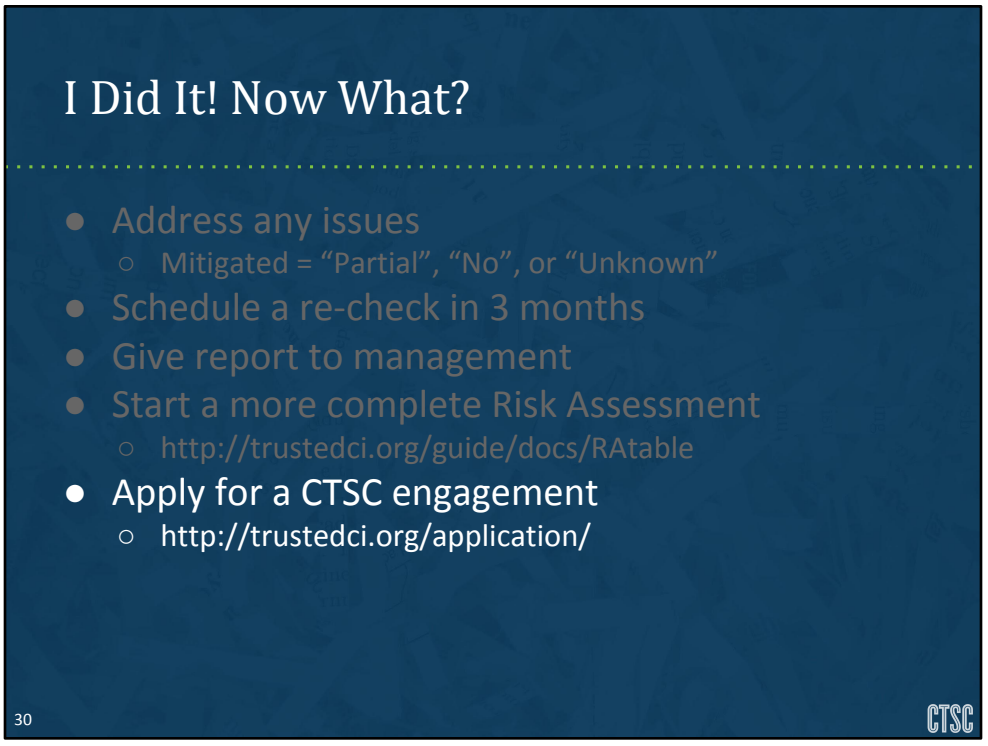
If you made it through the Risk Self-Evaluation spreadsheet and populated all the rows, congratulations! You have taken an important step toward addressing the cybersecurity readiness of your project. At this point you may be asking yourself, “now that I’ve filled out this spreadsheet, what can I do with it?” Here are few suggestions.

First and foremost, address any issues that may have been noted by the spreadsheet. This includes any answers in the “Mitigated” column marked as “Partial”, “No”, or “Unknown”. For issues that are partially mitigated or not mitigated at all, determine how much effort is necessary to change the answer to “Yes”. This may require man-hours or software not currently available to your project. If so, note this in the “Comments” column so you can re-evaluate in the future. For issues for which the mitigation is unknown, look for information sources either inside your project, or in the security community. CTSC has a discussion mailing list which might be a good place for you to post a question.

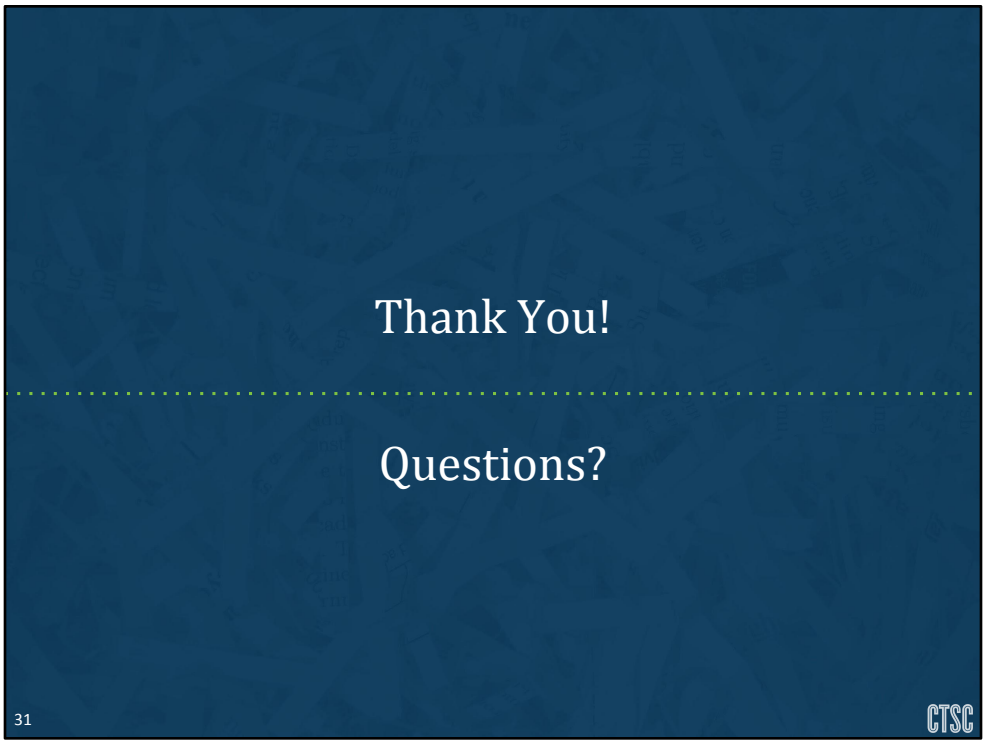
The Risk Self-Evaluation that you performed is a snapshot. It is possible that your project changes over time, whether due to new assets being added, or due to mitigations applied to risks pointed out by the spreadsheet. Unless you are one of the fortunate few whose project is static and with all risks successfully mitigated, it can be useful to re-evaluate your project on a quarterly basis. Since you have already done the hard work of performing the first Risk Self-Evaluation, future self-evaluations should be less onerous, and should hopefully yield more “Yes” responses for the “Mitigated” column.

The Risk Self-Evaluation can form the basis of a report to upper management on your project’s risk readiness. You could present the spreadsheet as-is, or you could use it as the basis for a simplified report on issues that should be addressed. Such issues could be presented as justification for the request of additional resources, for example.

For those projects which require a more full-featured Risk Assessment performed as part of an overarching Cybersecurity Plan, the Risk Self-Evaluation spreadsheet can be used as the starting point. The trustedci.org website has a Guide to Developing Cybersecurity Porgrams for NSF Science and Engineering Projects. This guide, based on NIST publications and frameworks, consists of several document templates and a Risk Assessment Table spreadsheet. The Risk Assessment Table spreadsheet is populated with your project’s assets and the associated threats, impacts, likelihoods, and controls. The spreadsheet serves as an aid when making decisions about assigning resources to reduce residual risk.



If the Risk Self-Evaluation pointed out issues that are too difficult or time-consuming for your project to address alone, CTSC may be able to help. As I said earlier, I have worked on several project engagements in the past, and I have used the Risk Self-Evaluation to help me at the beginning of these engagements. CTSC is now actively seeking engagees, and has a new application process available on the trustedci.org website. Potential engagees are asked to complete an online questionnaire to help determine if CTSC would be able to assist a project. Sending a completed Risk Self-Evaluation spreadsheet after completing the questionnaire would provide CTSC with additional information about your project and allow CTSC staff to make a better decision about the potential engagement.



If you made it this far through my presentation, I thank you for your attention, and I hope you have found some of the information useful to your project. I'll now open the floor to questions.

In case you haven't heard, this year's NSF Cybersecurity Summit is open to everyone. Visit trustedci.org/summit for online registration. Detailed program information is currently in development. The first day will consist of information security training sessions targeting both technical and managerial audiences. The second and third days will follow a workshop format with keynotes, panels, and face-to-face discussions. Participation in the summit is free, so please check the CTSC website for details on how to register.

(Jeanette gives closing remarks here.)

About the CTSC Webinar Series

To view presentations, join the discuss mailing list, or submit requests to present, visit:

http://trustedci.org/webinars

The next webinar is July 25th at 11am EDT

Speaker: James Marsteller

Topic: XSEDE Information Sharing

The CTSC Webinar Series is supported by National Science Foundation grant #1547272.

CTSC